Styrende dokumenter og informasjonssikkerhet - erfaringer fra Hydro

Sintef-seminar 22.november 2006

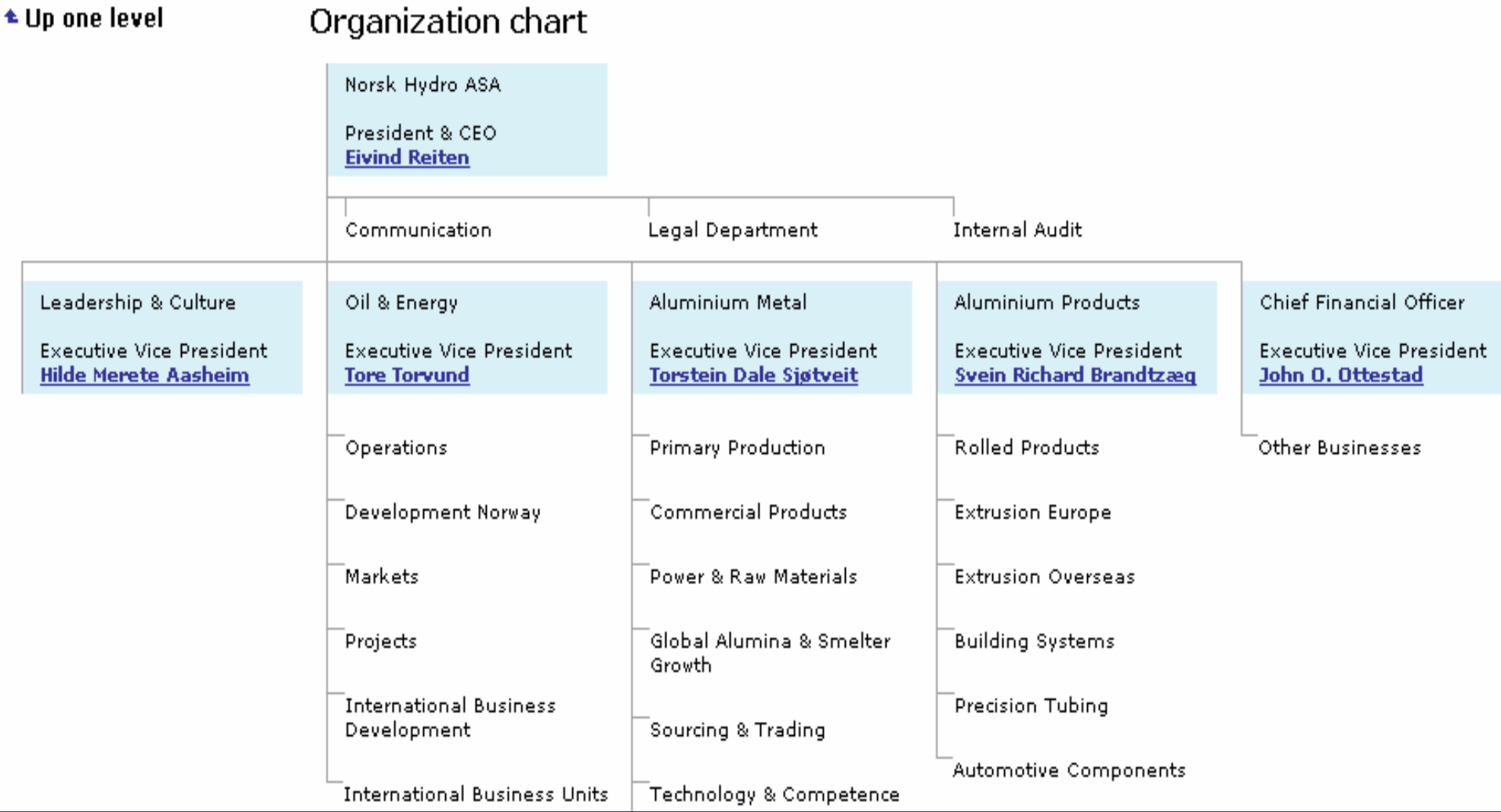
Hege Jacobsen
Hydro IS Partner, Norsk Hydro

2006-11-20

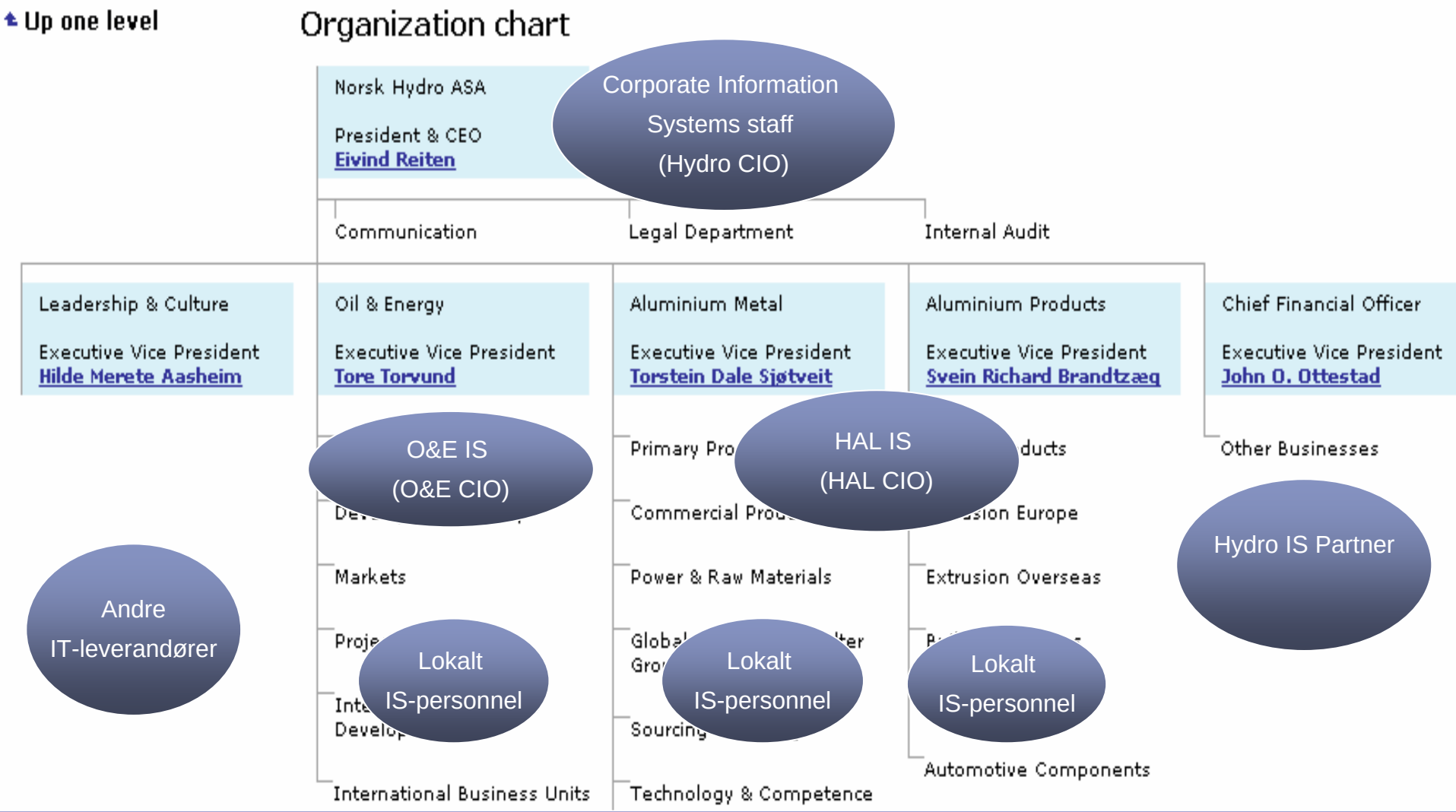
Innhold

- **Hydros organisasjon**
- **Målene for informasjonssikkerhet**
- **Ulike formål med styrende dokumenter**
- **Krav til policies for at de skal fungere**
- **Lærdom og anbefalinger**

Hydros organisasjon



Hydros organisasjon – fra et IS/IT-perspektiv

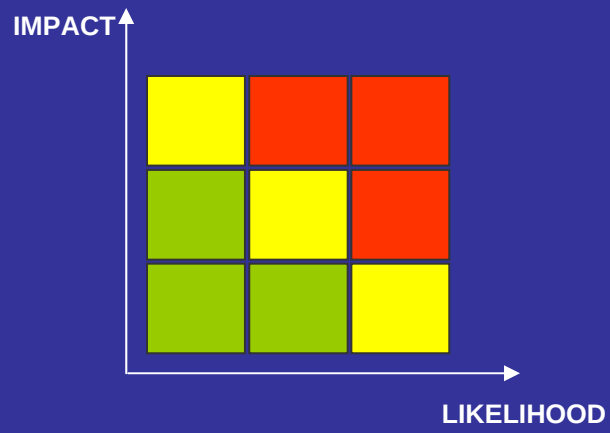


Hovedmål for arbeidet med informasjonssikkerhet

- **Beskytte Hydros informasjonsverdier**

Tilgjengelighet **Konfidensialitet** **Integritet**

- **Stanse kjente trusler og eliminere sårbarheter**
- **Finne et riktig nivå for informasjonssikkerhetstiltak**
- **Skape de riktige holdninger og ryggmargsreflekser**



HYDRO

Mekanismer i arbeidet med informasjonssikkerhet

- **Standarder og styrende dokumenter**
- **Bevisstgjøringskampanjer**
- **Risikoanalyser**
- **Kontroller og revisjoner**
- **Sikkerhetstjenester fra tjenesteleverandører**
- **Hendelseshåndtering**

HYDRO

Mekanismer i arbeidet med informasjonssikkerhet

- **Standarder og styrende dokumenter**
- **Bevisstgjøringskampanjer**
- **Risikoanalyser**
- **Kontroller og revisjoner**
- **Sikkerhetstjenester fra tjenesteleverandører**
- **Hendelseshåndtering**

HYDRO

Styrende dokumenter for informasjonssikkerhet

- **Corporate directive for Information systems**
  Føringer og målsetninger, organisering

- **Corporate procedure – Information security**
  Viktige prinsipper, roller og ansvar
  Hydros minstekrav for informasjonssikkerhet (Information security standard)

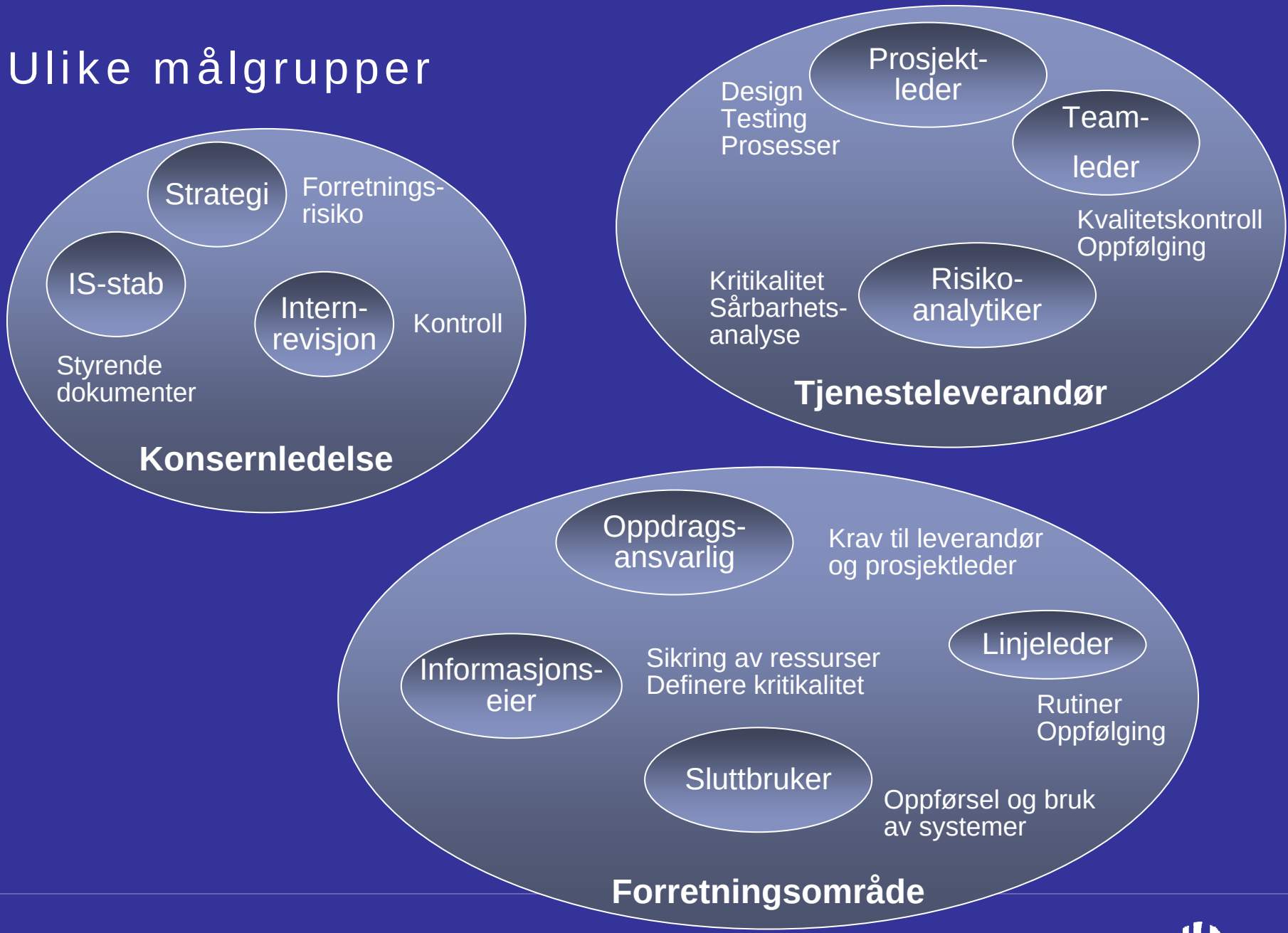
- **Spesifikke policies**
  - Internet and E-mail use policy
  - Information user standard
  - Password synchronization and single sign-on

- **Hydro IS architecture standard**
  Krav knyttet til spesifikke systemer

- **Relaterte styrende dokumenter**
  - Corporate directive for Health, Security, Safety and Environment
  - Corporate directive for Risk Management
  - Corporate procedure for
  - Sarbanes-Oxley act
  - Hydro IS Partner Management Systems Manual

HYDRO

Ulike målgrupper



HYDRO

Målsetninger for styrende dokumenter

- **Gi mandat og ansvar til ledere på ulikt nivå**
- **Gi kriterier for interne revisjoner og kvalitetskontroller**
- **Stille relevante krav til implementasjon og drift av IT-systemer**
- **Gi kunnskap om risikabel og riktig oppførsel**
- **Skape riktig forståelse og bevissthet om informasjonssikkerhet**

HYDRO

Styrende dokumenter må altså være

- **Presise og utvetydige formelt sett**
- **Ikke være generelle, men gi praktisk informasjon**
- **Gi klart formulerte krav knyttet til IT-faglige problemstillinger og trusler**
- **Virke relevante med lett forståelig argumentasjon**
- **Være komplette**
- **Være kortfattet**
- **Være teknisk korrekte, men forståelige av alle**

Uforenlige krav?

HYDRO

Utfordringer

- **Brukere kjenner ikke til policy-krav eller forstår dem ikke**
- **Brukere respekterer ikke policy-krav**
- **Policy-krav er for generelle, ikke tilpasset hver enkelt forretningsprosess og informasjonssystem**
- **Policy-krav blir sett på som kontraproduktive av linjen**
- **Linjen ser ikke sammenheng mellom egne interesser og policy-krav**

Med andre ord – policies blir pynt og papir ?

HYDRO

Lærdom i Hydro

- **Forenkling**
  - innhold, språk og struktur
  - Hydro er nå i ferd med å foreta en forenkling av sine policy-dokument
- **Styrende dokumenter må ikke inneholde mer enn man er villige til å stille organisasjonen til ansvar for**
  - Styrende dokumenter må klart formulere de enkelte aktørers ansvar
  - Ansvar må plasseres hos linjen
  - Følge opp med revisjoner og kontroller
- **Hensiktsmessig balanse mellom absolutte og kontekstuelle krav**
  - Risikoanalyser verktøy til å stille riktige krav til informasjonssikring
  - Mer fokus på riktige prosesser enn på bastante krav
- **Styrende dokumenter kan ikke stå alene**
  - Må følges opp av mer pedagogisk materiale rettet mot sluttbrukere
  - Må følges opp av kampanjer og kurs

HYDRO

- **Informasjonssikkerhet må henge sammen med andre ledelsesprosesser**
  - Enterprise risk management - knytte IT/IS til forretningsmessig risiko
  - Beslutningsprosesser – informasjonssikkerhet
  - Kvalitetssystemer

- **IT-aktører må være en fokusert målgruppe**
  - Prosjektledere, teamledere, leverandører er endringsagenter på dette området
  - Krav til IT-leverandører må bakes inn i service-avtaler (SLA)
  - IT-leverandørens egne kvalitetssystemer og interne kultur av sentral betydning
  - Oversettingen av policy-krav til praktiske løsninger ikke triviell – overlat ikke dette til teknikerne alene!

- **Ha fokus på sikkerhetspolicy-krav i systemutvikling**
  - Krav om risikoanalyser ved nye systemer og ved endringer i systemer eller bruksområder

Resultat – policies blir et redskap for proaktivitet og kontroll !

HYDRO

Spørsmål og kommentarer?

Hydro is a Fortune 500 energy and aluminium supplier with 33,000 employees in 40 countries. We are a leading offshore producer of oil and gas, the world's third largest aluminium supplier and a leader in the development of renewable energy sources. Our mission is to strengthen the viability of the customers and communities we serve.

HYDRO

Progress of a different nature

www.hydro.com